

⑨日本国特許庁(JP)

⑩特許出願公開

⑫公開特許公報 (A)

昭54-124653

⑪Int. Cl. ² G 06 F 15/30 G 07 F 7/10 G 07 G 5/00	識別記号 ⑫日本分類 97(7) J 1 115 D 0	庁内整理番号 7165-5B 6784-3E 6784-3E	⑬公開 昭和54年(1979)9月27日 発明の数 1 審査請求 有
----------------------------------------------------------------------	---------------------------------------	-----------------------------------------	------------------------------------------

(全 19 頁)

⑭取引端末装置

⑮特 願 昭54-22064
⑯出 願 昭54(1979)2月28日
優先権主張 ⑰1978年3月1日⑱米国(US)
⑲882529
⑳発 明 者 ロバート・ウィットコム・ア
ンダーソン
アメリカ合衆国カリフォルニア
州サン・ホセ・デザート・フレ
ーム・ドライブ6301番地
同 スティーブン・フランクリン・
ブロック

アメリカ合衆国カリフォルニア
州サン・ホセ・アンティカ・ド
ライブ5857番地
㉑発 明 者 メイ・リュウ・ギイ
アメリカ合衆国カリフォルニア
州サン・ホセ・コリブリ・コー
ト216番地
㉒出 願 人 インターナショナル・ビジネス
・マシーンス・コーポレーショ
ン
アメリカ合衆国10504 ニューヨ
ーク州アーモンク(番地なし)
㉓復 代 理 人 弁理士 頓宮孝一

明 細 書

1. 発明の名称 取引端末装置

2. 特許請求の範囲

ホストに接続することが出来、取引を承任する
為の取引端末装置において、

各々が暗号キーを含む、発行者に独特の複数個
の制御ブロックを貯蔵する貯蔵手段と、

値入が端末装置に呈示した識別カード上の、発
行者識別データ及びカード検証データを含む符号
化データを読取るカード読取手段と、

前記発行者識別データに回答して対応する制御
ブロックがあるかどうか前記貯蔵手段を探索する
手段と、

前記貯蔵手段の中に対応する制御ブロックが見
つからない時に前記符号化データを前記ホストに
連絡すると共に、前記貯蔵手段に書込む為の前記
ホストから対応する制御ブロックを受取る手段と、

前記対応する制御ブロックからの暗号キー・デ
ータに回答して前記カード検証データを暗号化し

てカード検査番号を発生する手段と
を有する取引端末装置。

3. 発明の詳細な説明

この発明は取引実行装置、更に具体的に言えば、
遠隔端末装置と連絡する中央データ・ベースを持
つていて、複数個の協働する機関の内の任意の1
つによつて発行された機械が読取り得る識別カー
ドに回答して、現金の支払又は資金の口座間の振
込みの様な取引の実行が出来る様にする取引実行
装置に関する。

公共の便宜並びに経済性の為、利用者から要請
された取引を実行する種々のシステムが開発され
ている。その一例は小切手現金化機である。この
機械は挿入された小切手からデータを読取り、小
切手が正しいと認められた場合、小切手の額に相
当する現金を支払う。クレジット・カードを使う
他のシステムも開発されている。

1つのクレジット・カード・システムは、中央
データベースにクレジット・カード口座情報を貯
蔵している。遠隔端末装置から口座番号が提示さ

れたことに応答して、システムが口座に関する情報を供給する。例えば、システムは、カードが切れていること、盗まれていること、又は残高を表示することが出来る。取引が完了した後、システムは貯蔵情報を正しく調節して、この取引の帳じりを合せる。

業務が混む時間又は時間外にその営業を拡張する為に廣々銀行によつて使われているクレジット・カード・システムの他の例では、端末装置を介して現金を支払い又は預金を受領することが出来る様にしている。典型的には、このような端末装置はクレジット・カードを受入れて、それから情報を読取る機構、キーボード、表示装置及び紙葉出入れ孔を含んでいる。端末装置はデータベースと共に動作することも出来るし、或いは単独の装置として動作することも出来る。各々のクレジット・カードに個人ID（識別）番号を与えることにより、人間が介在しなくても、現金の支払の際の安全性を高めることが出来る。この時、クレジット・カードによる取引は、クレジット・カー

(3)

発行したクレジット・カードを所定の端末装置で使える様にする場合、これら全ての銀行は同じ符号又はアルゴリズムを使うか、或いは口座データからID番号を導き出すのに使われるアルゴリズム関係を他の何等かの形で識別出来る様にしなければならない。この様な1つのシステムでは、各々の端末装置に同一の疑似乱数表を用意する。乱数表は、最初は機関の識別子で、次に表の出力と口座番号の数字との論理的な組合せによつて準不規則的にアドレスされる。このシステムでは、種々の銀行が発行したカードを使うことが出来るが、各々の銀行の人間は、その端末装置で他の全ての銀行が使うアルゴリズムに対する手がかりを持ち、銀行識別子符号が判つていれば、ID番号を容易に再生することが出来る。別のシステムでは、キーによつて作用するアルゴリズムを用意して、ID番号と口座番号との間の関係を決定する。このシステムでは、線形及び非線形操作を使つて、口座番号とキー番号とを組合せ、ID番号と比較される検査番号を発生する。米国特許第39566

(5)

ドから断取つた口座番号に対応するID番号がキーボードから送込まれた時にだけ出芽するようになる。この所要の対応性により、泥棒や単にクレジット・カードをみつけた者が、端末装置から現金を受取ることが出来ない様にする。端末装置がデータベースと一緒に作用する時、口座番号とID番号との間の対応性は無作為に選ぶことが出来るが、ID番号は予定の符号に従つて口座番号から導き出せる様にする場合が多い。この場合、ID番号を顧客による選択等によつて無作為に選べる様にする為に、カードには口座番号と共にずらし（オフセット）数値が記録される。このずらし数値は、予定の符号に従つて口座番号から導き出された番号に加えるか又はその他の形でそれと組合せた時、その結果が無作為に選んだID番号になる様に選ばれる。ID番号とカードの口座（並びにずらし）データとの間のこの予定の関係により、単独の端末装置が、ID番号をアルゴリズムによつて口座番号に関係づけることにより、ID番号を検査することが出来る。複数の協働する銀行が

(4)

15号にこのシステムが記載されている。然し、異なる銀行が発行したカードを同じ端末装置で使える様にするには、全ての銀行が同じキー番号を使わなければならないし、口座番号は全てのカードで同じフィールドになければならない。この米国特許のシステムを改良した1つの形式では、暗号キー表を各々の端末装置に用意しておき、表には、キーボードから送込んだID符号と比較する為の検査番号を発生する為に使われる口座、ずらし並びにその他のデータのカードのデータ・トラック上での位置を特定するデータと共に、複数の協働する銀行に対して、キー作用形アルゴリズムに使うのに必要なキーを入れておく。然し、このシステムはこの様な表の規模に対する貯蔵装置の制約を受け、各々の端末装置は、少数の選ばれた協働機関が発行したカードでしか動作することが出来ない。更に、このシステムは、銀行がその発行カードの基準を2つの異なる形式の間で変えている時に起る様に、機関のID及びカード状態が同一であつて形式が異なるカードに対処する

(6)

ことが出来ない。

表から導き出したキーによつて作用するクレジット・カード及びID番号確認方式は、各々の現金支払端末装置の安全性を改善すると共に他の銀行が発行したカードを引受ける点で、複数の銀行が協働出来る様にするが、端末装置に貯えられているか、或いは協働する銀行の口座にあつて、端末装置の動作によつて資金どうしの間の振込みが可能で大金の奪取をねらわれる弱点がある。重大な1つの問題は、単独動作が出来るか或いはオンライン動作も出来る端末装置の暗号アルゴリズムの安全性である。今日、現金支払端末装置の業務を行なう為には、非常に多数のオペレータ又は保守人員が必要である。例えば銀行の各支店の1人又は2人は、現金支払端末装置に内部接近することが出来る。こういう人員は、通常の保守の為に暗号キーにも接近出来る場合が多い。或いはその代りに、僅かな訓練しか受けていなくても、こういう人員は、内部回路の電気信号を測定することによつて、キーを入手する方法を覚える惧れが

(7)

データベースの口座内にある資金をだまして振込む惧れがある。

この発明の取引実行装置は、多くの口座に対する貯蔵情報のデータベースを持つホスト・データ処理装置と、複数の取引端末装置とを含む。各々の端末では、複数のカード発行者に対して暗号キー及びカード形式情報の表を保持しておき、取引を行なう許可を求める個人が端末装置に提示した識別カードから読取った発行者のIDに回答して、この端末装置の表を探索する。発行者のIDが端末装置の表に見つからない場合、端末装置がカード・データをホストに連絡すると、ホストがマスター表を同様に探索する。発行者に対するマスター表の項目は、取引に使う為、ホストから端末装置に連絡され、その後端末装置の表から追放することができる。ホストは消費者の情報のファイルを検査して、この情報の示す通り、カードを保存すること、取引を停止すること、又はその他の処置を端末装置に命令することが出来る。更に、局地のホストが別の遠隔のホストと連絡し

(9)

特開昭54-124653(3)

ある。一旦暗号キーが入手されれば、アルゴリズムが判ると、非常に多数の口座番号とID番号との間の対応性を作り出すことが出来る。その場合、カードの形式とカード上の検証データ及びずらしデータの場所とが判つていれば、カードのデータと無作為に選んだID番号との間の対応性を確かめることが出来る。

端末装置とホストのデータベースとの間で口座情報及びID情報を伝送することによつても、別の保安上の問題が起り得る。こういう伝送には、公共通信線路が使われる場合が多く、その為非常に多数の人間から監視される惧れがある。通信の安全性を改善する為に暗号が使われる場合が多いが、この符号を見破ることが出来た者、又は符号を入手することが出来た者は、この伝送を監視することにより、クレジット・カードの口座情報とID番号との間の対応性を導き出して、そのリストを編集することが出来るようになる。更に、偽の端末通信トラヒックを発生することにより、或る者がホストのデータベースに連絡をつけて、

(8)

て、端末装置からの取引の要請を予想して、局地のホストのデータベースに消費者の情報を入れておくことができる。

暗号キーはホスト及び端末装置の両方の表に暗号形式で貯蔵され、通信の時は2重に暗号化される。

暗号キー及びカード形式の表は、端末装置のカード読取機によつて決定されたカード・トラック状態に回答して、接近出来るようにする。

第1図について説明すると、この発明は、複数の銀行又はその他のカード発行機関によつて発行された個人識別カードを使って、複数の個人が自動銀行端末機等を作動することを許可する装置を提供する。各々の端末装置は、識別カードから読取ったデータと、個人がキーボードから送込んだデータとの間の対応性を検証する為に使う暗号キーを含む金融機関表(FIT)を備えている。端末装置のFITに項目を持っていない機関によつて発行されたカードが端末装置に提示された時、端末装置がホストCPUにあるマスターFITに

(10)

連絡することが出来るようにすることにより、F I Tは事実上規模が無制限である。

端末装置1は例えば交換システムにおける地理的に分散した複数個の自動銀行端末機(A T M)の内の1つである。こういうシステムでは、複数個の銀行が、他の銀行によつて発行されたA T Mカードを自分のものとして引受けることに合意する。

A T M1で銀行取引をしようとする個人が、磁気符号化カードをカード読取機2に挿入し、キーボード3から自分の個人識別番号(P I N)を送込む。カードから読取られた口座番号4又はその他の特定の有効認定データが暗号論理回路5によつて数に変換され、この数が比較器6でP I N7と対応するかどうか検査される。この検査並びに/又はその他の検査を充たすと、個人は所望の取引を進めることが許される。

各々の銀行は、その顧客に識別カード及びP I Nを発行する際、異なるP I Nキー k_1, k_2, \dots, k_m を使う。P I Nキーは、例えば口座番号

(11)

B Mシステム/370の様な汎用計算機、又はホスト及びサブホストの任意の組合せであつてよいが、これは後で更に詳しく説明する。

後述べるが、F I T表8及び10は一層多くの情報を持つていてよく、こうして独自のP I Nキーだけでなく、カードの形式、認可並びに取引パラメータを限定する融通性を各々の銀行Mに与えることができる。

第2図について説明すると、この発明の取引端末装置は、米国特許第3956615号に記載されている装置の改良である。この米国特許の第2図をこの出願の第2図として再掲し、参照し易くした。第2図の詳しい説明については、米国特許第3956615号を参照されたい。取引端末装置1をどの様な形で実現するかは、この発明を実施するのに重要ではないが、好ましい実施例が第2図に示されている。端末装置1は全体的にモジュール形であつて、情報母線62によつて端末装置の複数個のサブシステムに結合されたプログラム式マイクロプロセッサ60を含んでいる。マイ

(13)

から対応するP I Nを導き出す際に暗号論理回路によつて使われる多重ビット数である。F I T8に一组のこういうP I Nキー k_1, k_2, \dots, k_n (n 個の銀行又は異なる形式に対し)が貯蔵される。F I Tは、後で更に詳しく説明する様に、トラック状態の選定と共にカード読取機2が読取つた銀行識別フィールド9によつて探索され又はその他の形で呼出される、端末貯蔵装置のアドレス空間内の表である。全ての銀行又は形式に対するマスターF I T10をホストC P U11で管理し、そして端末のF I T8が、取引を完了する許可を要請する個人のI Dカードから読取つた銀行I D9に対応する項目を持つていない時、端末装置1によつてそのマスターF I Tが呼出される。ホスト11は、銀行I D9が取引会員のそれに対応することを検証し、そのF I T10の項目を端末装置1に連絡する。端末装置1は、この情報を現在並びに今後の取引に使う為、位置Nに貯蔵することが出来る。ホスト11は、I B M3600金融システム用のI B M3601通信制御装置又はI

(12)

クロプロセッサ60がクロック発生器64からのクロック信号によつて駆動され、電気的に変更し得る即時呼出し式記憶装置(R A M)及び読出専用貯蔵装置(R O S)の両方の機能を持つデータ貯蔵モジュール66に作動的に接続される。データ貯蔵装置66の内の読出専用貯蔵装置部分が、マイクロプロセッサ60用の種々の動作プログラムを貯蔵する。データ貯蔵モジュール66の即時呼出し式記憶装置部分が、プログラムの実行、キー並びにF I T表10の貯蔵用のスクラッチパッドになる。プロセッサ支援装置68、機械的な制御装置70、利用者通信装置72、現金支払装置74、オペレータ機能装置76及び通信装置78の動作特性については、米国特許第3956615号を参照されたい。

この発明の取引許可装置では、利用者の取引要請を実行する間、端末装置とホストとの間で6つの通信メッセージが必要になることがある。これらを第3図乃至第5図について説明するが、次の通りである。

(14)

V F I T 取引要請

V F I T 返答

V F I T 状態

取引要請

返答

状態

取引要請、返答及び状態メッセージは、米国特許第3956615号に記載されているものと同様であるが、この発明では変更が加えられている。V F I T メッセージは後に挙げた3つと略同じてあるが、取引端末装置1がF I T項目を得る為にホスト11に連絡しなければならない時に使われる。

この発明の取引実行装置は、ジ・アメリカン・バンカーズ・アソシエーション及び/又はスリフト・インダストリー・アソシエーションの2磁気ストライプ識別カード形式、及びインターナショナル・スタンダード・オーガニゼーション(I S O)が提案するトラック3磁気カード形式に合う様になつている。I D 番号とクレジット・カード

(15)

びP I N項目バイトが、端末装置によつて検出されたフラグ特殊状態に加えられる。T-2及びT-3は、カード読取機2が読取ることが出来る識別カードの磁気ストライプ上の2つの別々のデータ・トラックを表わす。

取引要請で、T-2及びT-3データのいずれか一方又は両方を伝送することが出来る。どのT-3フィールドを伝送するか並びにどの区域にある情報を送るかを記述するデータ・マップ・フィールドは発行者のP I N表項目にある。取引要請メッセージには下記のデータが含まれる。

メッセージの見出し

L — Lフィールドを含めて、メッセージの長さを表わす

N — 取引順序番号を表わす

C — メッセージのクラス/サブクラス(取引要請/通常又はV F I T取引)を表わす

(17)

情報との対応性を決定する特定の暗号アルゴリズム

は、この対応性が暗号キーに依存するものでなければならぬことを別にすれば、この発明を実施する上で重要ではない。米国特許第3956615号に記載されている暗号アルゴリズムはルツフと呼ばれているが、この発明の装置は、

Federal Register 第40巻、第52号(1975年3月17日、月曜日)所載のNational Bureau of Standardsの"Encryption Algorithm for Computer Data Protection"(以下DESと呼ぶ)を使うのに通している。

取引要請メッセージ

この発明では、米国特許第3956615号に記載されている取引要請メッセージに対して、次の拡張機能を加えられている。このメッセージは、取引の処理のためにホスト/サブホストに送られる普通の取引情報と共に、T-3及びT-2カード・データを伝送する。メッセージ・フラグ・バイト及

(16)

可変フィールド(V A R)

各々の引出し要請に対するロールオーバー式札計数器の合計。或いは取引順序番号

消費者P I N

消費者又は顧客が送込んだP I N

口座出フィールド

消費者のキーボードからの記入によつて定められた口座出フィールド

口座入フィールド

消費者のキーボードによる記入によつて定められた口座入フィールド

特殊取引番号フィールド

金額フィールド

札混合フィールド

T-2カード・データ

メッセージ・フラグ

ビット0 T-2は良好。

1 T-3は良好。

2 P I N再試行カウンットの限界に達する。

3 P I N再試行の取消し失敗。正しい

(18)

P I Nを送込まなかつた場合、このビットをセットして不完全取引要請が送られる。

- 4 I Dカードがカード読取機の輸送部の裏側に止まっている間に、スイッチの不規則性が検出された場合、カードのひつかかりが起つている恐れがあることを表わすスイッチ不規則性。
- 5 P I N未検査フラグ。端末装置がP I Nの検証をしない時、何時でもセットされる。
- 6 I Dカードにトラック2及び3の両方が検出されたことを表わす2トラック・カード。

P I N再試行

許される限界に達する前に、顧客が正しいP I Nを送込もうとした試行の回数を示す。

T - 3データ・マップ

T - 3カード・データ・フィールド中でどの

(19)

に、選択した各々のトラック(T 2、T 3)に対して送るべきデータ量を特定する。ホスト/サブホストは、適当なP I N表の項目を送ることによつて応答することが出来る。V F I T取引要請メッセージは下記のフィールドを含む。

メッセージの見出し

取引順序番号

メッセージ・フラグ

T - 2データ

T - 3データ

メッセージの見出し及びメッセージ・フラグ・フィールドは、取引要請メッセージに対して上に述べた様に特定される。

取引返答メッセージ

取引返答メッセージはホスト/サブホストが、動作、表示及びステートメント・プリンタ・データと共に、カードに書込む為にT 3データを送ることが出来る様にする。このメッセージは下記のフ

(21)

T - 3フィールドが送られているかを示す。

これはこの取引のI Dカードに対してP I N表の項目中に発見されるT - 3データ・マップの写しである。

T - 3カード・データ

T - 3カード・データは、それが首尾よく読取られ、且つP I N表の項目がそれを送るべきことを示す時に、伝送される。トラック情報の全部又は或るフィールドが、P I N表項目のT - 3データ・マップの指示により、伝送されることがある。

V F I T取引要請メッセージ

この特別の取引要請サブクラス(メッセージの見出し、前掲のバイトC)は、(初期プログラム挿入、I P Lで端末装置の初期設定の際)仮想P I N表項目機関連断権を選んだ場合、端末装置がホスト/サブホストに仮想P I N表項目要請をすることが出来る。この断権は、仮想P I N項目の要請を行なうことが出来るかどうかを特定すると共

(20)

フィールドを有する。

メッセージの見出し

計数器

ロールオーバー式札計数器の合計の値

動作

このバイトは、下記を含めて、端末装置がとるべき動作を特定する。

- 0 予め定められた利用者メッセージを表示する。
- 1 表示データ・フィールドにある利用者メッセージを表示する。
- 2 ステートメントを印刷する。
- 3 カード取出しの時間切れ。
- 4 取引を許可する。
- 5 クレジット・カードを保有する。
- 6 利用者の確認を要請する。
- 7 T - 3データを書込む。

数量1

ホッパ# 1から支払うべき札の数。ホッパが

(22)

1 台の端末装置ではゼロ。

数量 2

支払うべき札の数(ホッパが1台の端末装置)
又は貨幣ホッパ非2から支払うべき札の数。

表示データ

これがある場合、表示すべきメッセージ・データを含む。このメッセージは予め定められたメッセージの番号又は特別なメッセージの本文のいずれかであつてよい。

ステートメント・データ

これがある場合、取引ステートメントに印刷すべきデータ、即ち予め定められたメッセージ又は実際のメッセージ或いはその両方の番号。

T-3データ長さ

T-3データ・マップ

T-3データ

V F I T 取引返答メッセージ

この特別の取引返答メッセージは、端末装置か

(23)

- 4 P I N 項目をメッセージに入れる。
- 5 クレジット・カードを保有する。
- 6 処理の後に P I N 項目を追放する。

計数器 1

計数器 2

表示データ

P I N 項目

状態メッセージ/V F I T 状態メッセージ

状態メッセージが、取引返答メッセージに回答して、端末装置からホストに伝送され、返答メッセージで受取つたデータの処理結果を示す。この発明の好ましい実施例に関連する種々の状態ビットの定義は、取引の処理の不規則性並びに仮想 P I N 項目の返答の際の誤りに関する。状態メッセージに含まれる選ばれたフィールドは次の通りである。

メッセージの見出し

取引順序番号

計数器 1

(25)

ら要請された時、P I N 表の項目を伝送するものであるホスト/サブホストが P I N 項目を供給することが出来ない場合、V F I T 取引返答はゼロの P I N 項目フィールドを持つ。他の場合、動作バイトのビット 6 が 1 にセットされていなければ、新しい項目を受取るまで供給された P I N 項目を端末装置の記憶装置に保存する。P I N 項目は通信キー C 又はキー B に暗号化される。このメッセージは下記のフィールドを有する。

メッセージの見出し

計数器

ロールオーバー式札計数器の合計を端末装置に保管しておき、ホストの適用業務プログラムに保管する。

動作

- 0 予め定められた利用者メッセージを表示する。
- 1 表示データ・フィールドにある利用者メッセージを表示する。

(24)

データの長さフィールド

計数器 2

状態データ

- 0 T-3 零込み失敗
- 1 スイッチの不規則性
- 2 仮想 P I N 表の項目の誤り。このビットは次の場合にセットされる。
 - (1) 要請された項目が、発行者の I D の比較及びカードの種類に基づいて、送返された項目に合わない時
 - (2) 送返された項目が長すぎる時
 - (3) P I N 長さフィールドの値が所定の値より小さい時
 - (4) 送返された項目の長さがゼロの値である時、又は
 - (5) 項目が無効なフィールド位置の仕様を持つ時
- 3 T-3 データの誤り

次に第 3 図について説明すると、端末装置 1 で取引を行なおうとする個人が、磁気符号化クレジ

(26)

ット・カードをカード読取機2に挿入する。カードから読取られたデータがデータ貯蔵装置66に貯蔵され、局部F I T 8を探索する為にマイクロプロセッサ60によつて利用され、有効認定データ12、P I N検査番号15を作成するのに使わずにデータ13及び通信装置78によつてホスト11に伝送する為に取引要請メッセージ16に入れるデータを供給する。個人は、この取引の処理中の適当な時刻に、自分のP I N 7をキーボード3から送込む様に命令され、マイクロプロセッサ60内の比較器6でP I N検査番号15と比較される。

消費者カードがカード読取機2に正しく挿入された後、端末装置1は、取引に関する情報を見つけることが出来る様に、且つ消費者が送込んだP I Nを検証する次の工程を行なうことが出来る様に、カードから読取られたカード発行協会のI Dに対するP I N表(F I T)項目を探そうとする。マイクロプロセッサ60と協働してカード読取機2が行なうトラックの処理は、クレジット・

(27)

の探索は、カードが処理し得るものである場合、消費者が挿入したカードに対応するP I N表の項目を探す試みである。P I N表探索アルゴリズムは、発行者識別子(I I)を探索指数、クレジット・カードのトラック状態を修飾子として使う。探索指数は、I S O基準案T 3形式に従つて、カード番式I D、業界I D、標準発行者I D及び消費者の主要口座番号を含む20個までの連続的なディジットを含むことが出来る。F I T項目が第6図に示されており、後で説明するが、これを次の様に探索する。P I N表、又はF I Tに特定されている項目種類がカードの種類に合わない場合(例えばT - 2が良好で、T - 3がクレジット・カードで検出されないが、P I N表の項目がT - 3だけ、T - 2又はT - 3独立又はT - 2/T - 3の組合せである場合)、P I N表の項目を飛ばす。カードの種類がP I N表の項目の種類に合うと、P I N表の項目の定義を使つて、P I N表の項目中にある発行者I Dと比較するカード・データを突止める。それらが合わない場合、次のP I

(29)

カードを読取つて、それがトラック状態に基づいて処理し得るものであるかどうかを判定する。消費者がカード読取機2にカードを挿入する時、トラックが読取られ、必要であれば、各々のトラックに対するトラック状態を判定する為に再び読取られる。状態は良好、不良又は検出不能であることがある。少なくとも1つのトラックが良好状態であれば、カードは使用可能と考えられる。

交換システムの各々の独特な発行者が、P I Nの有効認定及びP I Nの暗号化に使うP I Nキーを供給する。こういうP I Nキーは、初期設定(I P L)の際、ホスト11から端末装置1に伝送される独特なP I N表8の項目として、交換所の会員機関によつて供給される。この代りに、これらの項目は、仮想P I N処理の為、ホストのF I T 10(第4図)に保持してもよい。

局地のF I T 8を探索する際にマイクロプロセッサ60が行なう工程が、第8図に示されている。V P I N処理の要請に回答して、ホスト11が同じ工程をとることが出来る。P I N表8、10

(28)

N表の項目に対して同じ過程が繰返される。合致すると、探索が終了し、P I N表8のその項目の定義を消費者の取引の残りの処理に使う。普通の項目がこのカードの種類に対してみつからず、仮想P I N表の項目の選択権が特定されていない場合、探索はP I N表8の最後の項目で終了する。合うものが見つからないと、クレジット・カードは消費者に返される。

普通の(即ち対応する)項目がF I T 8に見つからず、端末装置1に対して仮想P I N表の選択権が特定されている場合、マイクロプロセッサ60はV F I T取引要請メッセージ17を組立ててホスト11に伝送する。ホスト11は、ホストのF I T 10を探索し、F I T表の項目19を含むV F I T返答メッセージ18を組立て、端末装置1がF I T 8又はデータ貯蔵装置60の他の或る領域に貯蔵する様にする。この為、ホスト/サブホスト11にV P I N表の項目を要請する前に、前のV P I N要請で内部で保管してあつたV P I N項目を、現在のI Dカードと合うか、どうか検

(30)

査する。ホストのF I T 1 0に項目が見つからない場合、その事実が、V F I T取引返答メッセージ中の動作バイトのビット4によつて表示される。

消費者のクレジット・カードのデータに対応するP I N表8の項目が見つかった後、その項目を検査して、端末装置1又はホスト11のどちらによつてP I N有効認定を行なうかを判定する。ホスト11によるP I N有効認定が特定されている場合、トラック状態が検査されるが、端末装置1ではこれ以上P I Nの処理が行なわれない。トラック状態が不良トラックであることを表わし、P I N表の項目が「不良トラックを持つカードを排除せよ」を特定する時、取引は停止し、カードが消費者に返され、適当なメッセージが表示される。カードが不良トラックを持っていないか、或いはP I N表の項目が「不良トラックを持つカードを処理せよ」を特定する場合、P I Nの処理が進められる。

暗号アルゴリズム20で、P I N表8からの暗号化されたP I NキーがキーAを使つて復号され、

(31)

F I T項目の内の下記のパラメータが、カード・データに対する長さ、変位及び埋合せの仕様と、10進化表と、P I N検査を行なうのに必要な暗号キーとを定める。

V A L D I S Pは、カード・データの最初のデータ・ディジットからの有効認定データ・フィールドの変位を定める。

V A L L E Nは、有効認定データ・フィールド中に含まれるディジットの数を定める。

V A L P A Dは、ディジット数が16未満である場合、有効認定データの埋合せに使われるディジットを定める。

O F F D I S Pは、カード・データの最初のデータ・ディジットからのずらしデータのフィールドの変位を定める。

C H R L E Nは、ずらしデータ・フィールドに含まれるディジット数、顧客が送込んだP I Nで検査するディジット数、及び顧客が送込んだP I Nに許されるディジットの最小数を特定するパラメータである。

(33)

後で説明する暗号化工程5に使うP I Nキーを発生する。P I N検査又は有効認定データ12及びずらしデータ13は、いずれかのトラックT-2又はT-3の何処にあつてもよい。端末装置のP I N有効認定がP I N表の項目によつて特定されている場合、その位置はP I N表の項目によつて記述されている。端末装置1によるP I N処理はマスター・キー(カード・データ、カードに対して選ばれたF I T項目からのデータ、及び消費者が送込んだキーボード・データ)を含む。マスター・キーがマスター・キー装入指令で、ホスト11から端末装置1に送られる。マスター・キー装入指令が実行されていない場合、オペレータ/C Eパネル76から送込んだAキーをマスター・キーとして使う。有効認定データ12は消費者の口座番号であつてもよいし、或いは金融機関が消費者を同定する為に使いたい任意の数であつてもよい。ずらしデータは随意選択であり、消費者が送込むP I N及び有効認定データを独立に特定することが出来る様に選ぶことが出来る。

(32)

D E C T A Bは、暗号化された有効認定データを10進数に変換する為に使われる16個の10進ディジットの表である。

E P I N K E Yは、有効認定データを暗号化する為に使う暗号化されたP I Nキー(マスター・キーで暗号化される)である。

キーボード3から下記のデータが送込まれる。

P I Nは顧客によつてキーボード3から送込まれた個人識別番号である。

P I N長さは、顧客が送込んだP I Nにあるディジットの数である。

次に第3図について説明すると、端末装置1はホストから切離されたP I N検査を次の様に行なう。

1. V A L D I S Pを使つて場所を見つけ、V A L L E Nを使つて長さを決定することにより、カードから有効認定データ12を求める。

2. 有効認定データ・フィールドにあるディジット数を表わすV A L L E Nが16未満である場合、V A L P A Dによつて特定されたディジット

(34)

を使つて、埋合せ工程21で、16ディジットの右側に有効認定データ12の埋合せを行ない、埋合せ有効認定データ22を作る。

3 下記の2つの方法のどちらかにより、PINキーを求める。

FIT表の項目中にEPINKEY(又はFITキー)パラメータが特定されている場合、マスター・キーを使つてEPINKEYの値を復号する。

FIT表の項目中にEPINKEYパラメータが特定されていない場合、マスター・キーをPINキーとして使う。

4 PINキーを使つて、暗号アルゴリズム5によつて埋合せ有効認定データ22を暗号化し、暗号化有効認定データ23を作る。

5 DECTABを使つて、暗号化有効認定データ23を10進化ルーチン24で10進ディジットに変換し、10進化有効認定データ25を作る。暗号化有効認定データ23の各々の16進ディジットがDECTABからの10進ディジット

(35)

9 PIN検査番号15を比較器6で、顧客が送込んだPIN7のディジットと右側からディジット毎に比較する。比較が成立する為には、PIN検査番号15の全てのディジットは、顧客が送込んだPIN7の対応するディジットと同じでなければならない。顧客が送込んだPIN長さがCHKLENより大きければ、顧客が送込んだPIN7の一番左側の(最初に送込んだ)ディジットは検査されない。こういう余分のディジットは任意の値であつてよい。比較6が成立する場合、端末装置1は、データを起立て、その一部分をホスト11に対する取引要請メッセージ16に暗号化することにより、取引を進める。比較6が成立しない場合、端末装置1は試行設定パラメータによつて定められる様に、顧客に0回又は更に多くの試行を許す。端末装置1はカードを戻し、ホスト11にメッセージを全く送らないで、取引を停止することが出来る。この代りに、端末装置1はホスト11に無効PIN取引要請メッセージを送り、カードを戻すか又は保有し、場合によつては顧客

(37)

に替えられる。選ばれた10進ディジットは、DECTAB中のその変位(0-15)が、有効認定データ23中で取替えられる16進ディジット(0-F)の数値に対応するディジットである。

6 OFFDISPを使つて場所を探すと共に、CHKLENを使つて長さを決定することにより、カードからずらしデータ13を求める。OFFDISP=255(X'FF')である場合、ずらしデータに全部ゼロのディジットを使う。

7 ブロック26で、ずらしデータ13を10進化有効認定データ25と揃えて、ずらしデータ13の一番左のディジットが10進化有効認定データの一番左のディジットより0個又は更に多くのディジット位置だけ右へ変位する様にする。この変位のディジット位置の数は、PIN長さからCHKLENを差し引くことによつて求められる。

8 ずらしデータのディジット13をそれと揃っている10進化有効認定データのディジット25と基数10でディジット毎に加算する。その結果がPIN検査番号15である。

(36)

に対してメッセージを表示する様に端末装置1に指示する取引返答を待つ。

第4図には、端末装置1からのVFIT取引要請17を処理する場合のホスト/サブホストが示されている。前掲米国特許第3956615号の第4図に説明されている手順に従つて、VFIT取引要請メッセージ17を復号する。局部FIT表8の探索について前に述べた様に(並びに第8図に示す手順に従つて)、トラック状態及び発行者識別符号を使つて、付属データ処理装置11がサブホストFITを探索し、通信キーB又はCを使つて、暗号アルゴリズム28で暗号化する為、対応するFIT項目19を突止める。暗号アルゴリズム28は、Federal Register、第40巻、第52号(1975年3月17日、(月曜日)号)に記載されているData Encryption Standards (DES) of the National Bureau of Standardsに従つて、付属データ処理装置11又はデジタル・ハードウェア論理装置によつて実行される適用業務プログラム

(38)

として実現することが出来る。

V F I T取引要請メッセージ17中に、I Dカードからのトラック・データとして供給される顧客口座識別データを使つて、付属データ処理装置11がその顧客データ・ファイル29を探索することが出来、そこに貯蔵されている情報に基づいて、V F I T返答メッセージ18中の動作ビットを通じて、カードを保有するか又は取引を停止するか又は取引を承認する様に、端末装置1に命令することが出来る。同様に、付属データ処理装置は、表示メッセージ・ファイル30からV F I T返答メッセージ18に表示データを入れることが出来る。更に暗号アルゴリズム28がV F I T返答メッセージ28の一部分31を暗号化する。随意選択による表示データがない場合、この結果F I T項目19の一部分が2重に暗号化されることがある。F I T表10に貯蔵されているP I Nキーが、マスター・キーを使つて既に暗号化されているから、この結果2種類の異なるキーを使つて、F I T項目19が3重に暗号化される可能性がある。

(39)

口座ファイルに一括処理する為に、自分自身の顧客に対する取引データを顧客データ・ファイル29にアセンブルするだけでよい。この後、取引要請メッセージを端末装置1からサブホスト11が受取つた時、この要請を処理する為に必要な全てのデータは、初めからあるにしても、或いはホスト27から求めたものにしても、そのファイル29から利用し得る。

この発明の別の実施例として、端末F I T 8は、端末装置1を所有するか又はその他の形で管理する銀行の種々の書式だけに対する項目と、主体F I T 10が管理する協働する銀行に対する全てのF I T項目とを貯蔵し、こうして銀行員又はその他によるF I T 8の呼出しにつき、システムの保安性を高めることが出来る。所定の銀行に対するF I T項目は、1回の取引を実行する間、端末装置1に保存してあればよく、その後追放する。

この発明の更に別の実施例として、銀行がその発行カードの基本を成る書式から別の書式に変えることが出来る。この変更の際、同一の機関I D

(41)

付属データ処理装置11は主体データ処理装置27にも接続し得る。これは銀行の中央のホスト、交換所システムの全ての会員に対する中央のホスト、または適当な交換通信リンクを介してサブホスト11から連絡し得る交換所システムの別の会員のホスト又はサブホストであつてよい。

付属データ処理装置11は、V F I T取引要請メッセージ17から得られた機関I D及びトラック状態に対するF I T 10内の対応する項目を含めて、V F I T返答メッセージ18を端末装置1に通信する手段になる。取引要請メッセージを発生する端末装置1内でのデータ処理と並列に、サブホスト11は主体データ処理装置17を呼出して、前にV F I T取引要請メッセージで通信したデータ中に確認された個人に対し、端末装置1から取引要請を受取ることを予想して、その顧客データ・ファイル29に装入する為に、消費者ファイルを求めることが出来る。この為、付属データ処理装置11は、自分が発行したカードに対する顧客データ・ファイルを管理するか、或いは後で他の

(40)

及びトラック状態を持つカードが相異なる2つの書式に関係するのが普通である。符号化トラックにある他のデータを検査する能力のない端末装置1は、その区別が出来ない。こういう場合、発行銀行は、サブホスト11にそのF I T項目だけを管理し、端末装置1が、その発行者に対して顧客から要請された全ての取引を処理する為に、V F I T取引要請メッセージを通じて連絡することを要求する様にすることが出来る。サブホスト11では、適用業務プログラムを設けて、カードの書式を同定するフィールドから読取つたデータの全ての部分或いは他の或る部分を検査し、こうしてサブホスト11が、取引が完了した時、端末装置1の貯蔵装置からそれを追放せよと言う指令と共に、適切なF I T項目を端末装置1に供給出来る様にする。

従つて、以上の説明から判る様に、端末装置1は、それ自体が別の遠隔ホスト27に接続されたサブホストであつてもよいホスト11に接続することが出来、こうしてデータの保安をはかれるよ

(42)

うにすると共に、F I T表8、10及びファイル29の様な顧客口座ファイルを多数の場所に分配することにより、処理及び貯蔵の効率をはかることが出来る。端末装置1に対してV F I T返答メッセージ18で返答しながら、ホスト27からの口座データをデータ・ファイル29に入れることにより、ホスト11は、端末装置1から予想される取引要請に対して、一層敏速に回答することが出来る。

ホスト11は例えばIBM3601制御装置又はIBMシステム370データ処理装置であつてよい。ホスト27はIBMシステム370であつてよい。ホスト11は、遠隔ホスト27に接続される時はサブホストと呼び、その他の時はホストと呼ぶ。いずれの場合も、ホスト及びサブホストと言う言葉は、端末装置1のインターフェイスとして使われる時、互換性を以つて使われる。

次に、第6図について、P I N表の項目を説明する。P I N表の項目には基本的に3種類ある。T - 2 (T - 2のみ又はT - 2独立)、T - 3 (

T - 3のみ又はT - 3独立)及びT - 2 / T - 3組合せである。項目は表の中で任意の順序で現われ得る。違う種類の項目は同じ発行者I Dを持つが、T - 2及びT - 3独立は組合せT - 2 / T - 3とは相互に排他的である。これらの項目の種類その他に、共通P I N表項目を特定することが出来る。共通項目は、特定する場合、P I N表の最後であり、P I N表の項目の合うものが見つからなかつたクレジット・カードに対して使われる。P I N表の項目は、発行者I Dの場所以外、消費者I Dの検証に必要な全ての情報を含む。発行者I Dの場所は任意の取引の前にホスト11によつて端末装置1に供給される設定イメージから得られる。裏づけのある各々のカードの種類 (T - 2、T - 3、T - 2 / T - 3) に対して、F I T表8、10に別の小項目が必要である。次に共通部分40のフィールド41 - 49を説明する。

(43)

共通部分

項目41の長さ

このバイトを含むP I N項目の全部の長さ
フラグ42

- ビット0 = 1 トラック2だけが支援されている。
- ビット1 = 1 トラック3だけが支援されている。
- ビット2 = 1 トラック2独立が支援されている。
- ビット3 = 1 トラック3独立が支援されている。
- ビット4 = 1 T - 2 / T - 3が支援されている。
- ビット5 = 0 Ⅱがトラック2上にある。
 = 1 Ⅱがトラック3上にある。
 ビット4 = 1の時だけ使う。
- ビット6 = 0 1つの不良トラックを持つ
 T - 2 / T - 3カードを処

(45)

(44)

理する。

- ビット6 = 1 1つの不良トラックを持つ
 カードを排除する。ビット
 4 = 1の時だけ使う。

発行者P I Nの長さ43

発行者が受理する最大のP I Nの長さ。許容し得る最小値は4である。

P I N検査の長さ44

端末装置によつて有効と認定されるP I Nのディジット数。ゼロであれば、P I Nの検証は行なわない。

発行者P I Nパッド/検査パッドのディジット45

ビット0 - 3は、消費者が送込んだP I Nが16ディジットより少ない場合、端末装置で使われる組合せディジット。DES暗号化の為、消費者が送込んだP I Nの右に埋合せをして16ディジットにする。ビット4 - 7は、発行者が供給したP I N検査データが16ディジットより少ない場合に使う埋合せディジットであり、カードから

(46)

のPIN検査データの右側に組合せ、DES暗号化用の16デジットにする。

PINキー46

PINの暗号化並びにPINの有効認定の為に使われる、発行者が供給したキー。PINキーはマスター・キーで暗号化される。

10進変換表47

PINの有効認定に使われる発行者から供給される表。クレジット・カードのPIN検査データの暗号化により、16個の16進デジットが発生されるが、これを10進デジットに変換しなければならない。各々の16進デジットは10進デジットに置換えられるが、この表(0-15)内でのその位置が、取替えようとする16進デジットの値(0-F)に対応する。変換が行なわれたら、必要な場合、変換結果にずらし値を加え、次に計算したPINと消費者のPINとの比較を行なう。

発行者IDの長さ48

(47)

PIN項目のフィールド51に特定された、フィールド分離子の値からカード上のPIN検査データまでの変位。顧客が送込んだPINとの相関の基準として使う。

発行者PIN検査データの長さ54

カードに記されたPIN検査データの長さ。16デジットより短い場合、端末装置によつて右側に埋合せデジットを加え、DES暗号化用の8バイトのフィールドにする。

次にT-3のみ部分のフィールド91-97及びT-3独立フィールド90を説明する。

PINずらし及びPIN検査の位置91

ビット0-3はPINずらし、T-3までのフィールド分離子の数。ビット4-7はPIN検査データ、T-3までのフィールド分離子の数。

発行者PINずらしの変位92

PIN項目のフィールド91に特定された、フィールド分離子の値からトラック上のP

(49)

IDフィールドのバイト数で表わした長さ。

発行者ID49

これは、PIN表の項目の選択に使われる発行者IDを含む。発行者IDフィールド全体がX'FF'であることは、共通PIN表現項目を表わす。これはPIN表の最後の項目でなければならない。

次に、T-2のみ部分のフィールド51-54とT-2独立フィールド50を説明する。

PINずらし及びPIN検査の位置51

ビット0-3は、PINずらしT-2に対するフィールド分離子の数。ビット4-7は、PIN検査データT-2に対するフィールド分離子の数。

発行者PINずらし変位52

PIN項目のフィールド10に特定された、フィールド分離子の値からトラック上のPINずらしまでの変位。このフィールドがX'FF'であれば、ずらしは用いない。

発行者PIN検査データの変位53

(48)

INずらしまでの変位。このフィールドがX'FF'であれば、ずらしは用いない。

発行者PIN検査データの変位93

PIN項目のフィールド91に特定された、フィールド分離子の値からカード上のPIN検査データまでの変位。顧客が送込んだPINとの相関の基準に使う。

発行者PIN検査データの長さ94

カードに記されたPIN検査データの長さ。16デジットより短い場合、端末装置によつて右側に埋合せデジットを加え、DES暗号化用の8バイトのフィールドにする。

T-3PIN再試行の位置95

ビット0-3はあてである。ビット4-7はT-3PIN再試行カウントを含むカード上のフィールドまでのフィールド分離子の数。

T-3PIN再試行の変位96

カード上のフィールド内のT-3再試行カ

(50)

ワントの変位。

T-3データ・マップ97

T-3内のどのフィールドを取引要請メッセージで送るかを示す。

次にT-2/T-3部分100のフィールド101-107を説明する。

PINずらし及びPIN検査の位置101

ビット0-3は、フィールド102に特定されたトラック上のPINずらしまでのフィールド分離子の数。ビット4-7は、フィールド103に特定されたトラック上のPIN検査データまでのフィールド分離子の数。

発行者PINずらしの変位102

ビット0はPINずらしトラックの位置。
ビット1-7はPIN項目のフィールド101に特定されたフィールド分離子の値から、トラック上のPINずらしまでの変位。
このフィールドがX'FF'であれば、ずらしは用いない。

(51)

は、消費者の随意選択によつて再試行カウントが使われる。

T-3データ・マップ107

T-3内のどのフィールドを取引要請メッセージで送るかを示す。

第7A図及び第7B図には、この発明の取引実行装置を実施する最適な様式による動作が例示されている。顧客IDカードを110で読取り、トラック状態並びに発行者の識別符号に応じて、対応するFIT項目について、局地FIT表の探索が111で行なわれる。FIT項目が112で見つかり、取引データがカードから並びにキーボードで送られたものから113の所で収集され、ホストに通信(114)する為の取引要請メッセージを作成する。ホストでは、顧客口座ファイルを検査し、取引の以後の実行に関する命令を含む取引返答メッセージが115の所で端末装置に送返される。端末装置は命令を実行し、顧客口座ファイルを適切に更新することが出来る様に、どういふ処置をとつたかをホストに知らせる状

(53)

発行者PIN検査データの変位103

ビット0はPIN検査データのトラックの位置。ビット1-7は、PIN項目のフィールド101に特定されたフィールド分離子の値から、カード上のPIN検査データまでの変位。消費者が送込んだPINとの相関の基準に使う。

発行者PIN検査データの長さ104

カードに記されたPIN検査データの長さ。
16デジットより短い場合、端末装置によつて右側に埋合せデジットが加えられ、DES暗号化用の8バイトのフィールドにする。

T-3PIN再試行105

T-3PIN再試行カウントを持つカード上のフィールドまでのフィールド分離子の数。

T-3PIN再試行の変位106

カード上のフィールド内のT-3再試行の変位。このフィールドがX'FF'であれば

(52)

態メッセージ116をホストに送返す。

顧客IDカードのデータに対応するFIT項目が局地FITの探索で見つからなかった場合、端末装置が、ホストに対するVFIT取引要請メッセージに必要なデータを117の所で収集する。このVPINデータ収集手順は第9図のフローチャートに示されている。この第9図は、VPINを選択したホストから前に提供された制御128に回答するT-2及びT-3データの選択130-133を示す。

端末装置がホストに対してVFIT取引要請を118の所で連絡し、ホストはそのファイルから暗号化されたVFIT項目を持つ取引返答119をアセンブルする。端末装置が120の所でVFIT項目を有効と認定し、VFIT項目が要請したものに合うか、或いはその他の形で受理されたというVFIT状態メッセージを121の所でホストに連絡する。カードを保有し並びに/又は取引を停止する様にVFIT取引返答メッセージで命令されない場合、端末装置は取引データの収集

(54)

に準み、要請を実行する。V F I T取引返答メッセージでそうする様に命令された場合、取引の実行が完了した時、端末装置はホストから受取つたV F I T項目を、その局地F I T表から1 2 2、1 2 3の所で追放する。

この発明の取引実行端末装置並びに取引実行装置は、金融機関の顧客に対して、セルフサービスの能力を持たせる。この端末装置を使うことにより、銀行員の助けを借りずに、然も一日24時間、多くの銀行機能の取引が出来る。識別データを符号化した磁気ストライプ・カードが金融機関によつて顧客に対して発行され、顧客はこれを使つて、端末装置で取引を開始する。顧客の身元は個人識別番号(P I N)によつて検証される。顧客はこの番号を端末装置のキーボードから送込む。

識別データを含む慎重な扱いを要するデータは、その保安を保つ為に暗号化される。暗号化並びにその後の復号は、暗号アルゴリズム及び金融機関の秘密暗号キーを用いて行なわれる。装置の暗号アルゴリズムは、前に述べたThe National

(55)

4.図面の簡単な説明

第1図はこの発明の取引実行装置を表わす機能ブロック図、第2図は第1図に示した取引実行装置に使われる取引端末装置の機能ブロック図、第3図は利用者によつて開始された取引要請が最初は取引端末装置によつて処理される様子を示す動作ブロック図、第4図は第1図に示した取引実行装置に使われる付属/遠隔主体データ処理装置の機能ブロック図、第5図は取引実行装置の機能ブロック図で、典型的な取引の進行中に、取引端末装置とホスト又はサブホスト・データ処理装置とで交される通信メッセージを示す。第6図はホスト/サブホスト・データ処理装置及び取引端末装置に貯蔵される金融機関表の機能ブロック図、第7A図及び第7B図はこの発明に従つて取引端末装置によつて行なわれる工程を示す動作フローチャート、第8図は第7図のF I T探索工程の動作フローチャートで、第4図のサブホストの金融機関表を探索する際に行なわれる工程をも示す。第9図は第7図のV P I Nデータ収集工程の動作フ

(57)

Bureau of Standards のData

Encryption Standards (DES)として提案されたアルゴリズムに選ぶことが出来る。

端末装置は交換所形式で使うことが出来る。即ち、参加した多数のカード発行機関からのカードの所有者が同じ端末装置を使う様にすることが出来る。

顧客の取引を処理する際に使われるデータの表を端末装置に管理しておき、多くの協働するカード発行機関に対する項目を、顧客のカードから読取る機関識別子によつて呼出す。その表の探索によつて合う項目が見つからない場合、ホストに対して要請メッセージを送り、ホストに管理しているマスター表から合う項目を要請する。マスター表の項目を端末装置で使つた後、それを追放することが出来る。こうして、システムの安全性を高めることが出来る。ホスト(又はサブホスト)の消費者ファイルは、端末装置からの取引要請を扱う為にホスト(又はサブホスト)に消費者ファイルを入れることが出来る。

(56)

ローチャートである。

2...カード読取機、5...暗号化装置、8...金融機関表、11...ホスト、78...通信装置。

出 願 人 インターナショナル・ビジネス・マシーンス・コーポレーション
復代理人 弁理士 頼 官 孝 一

(58)

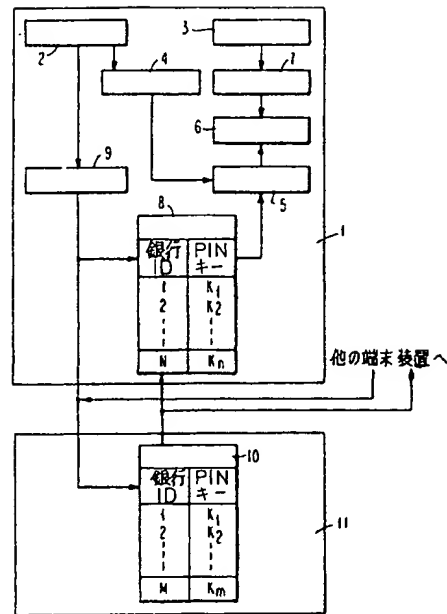


FIG. 1

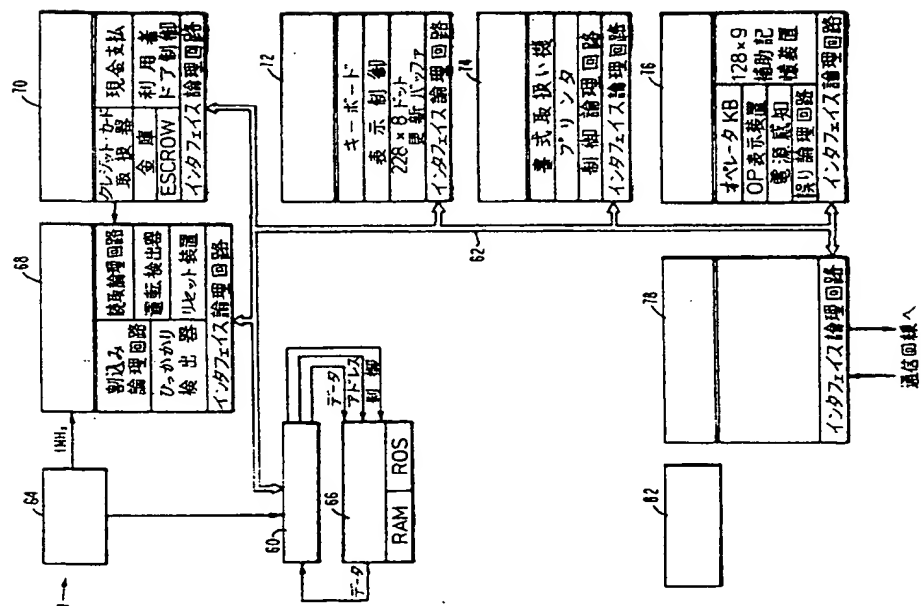


FIG. 2

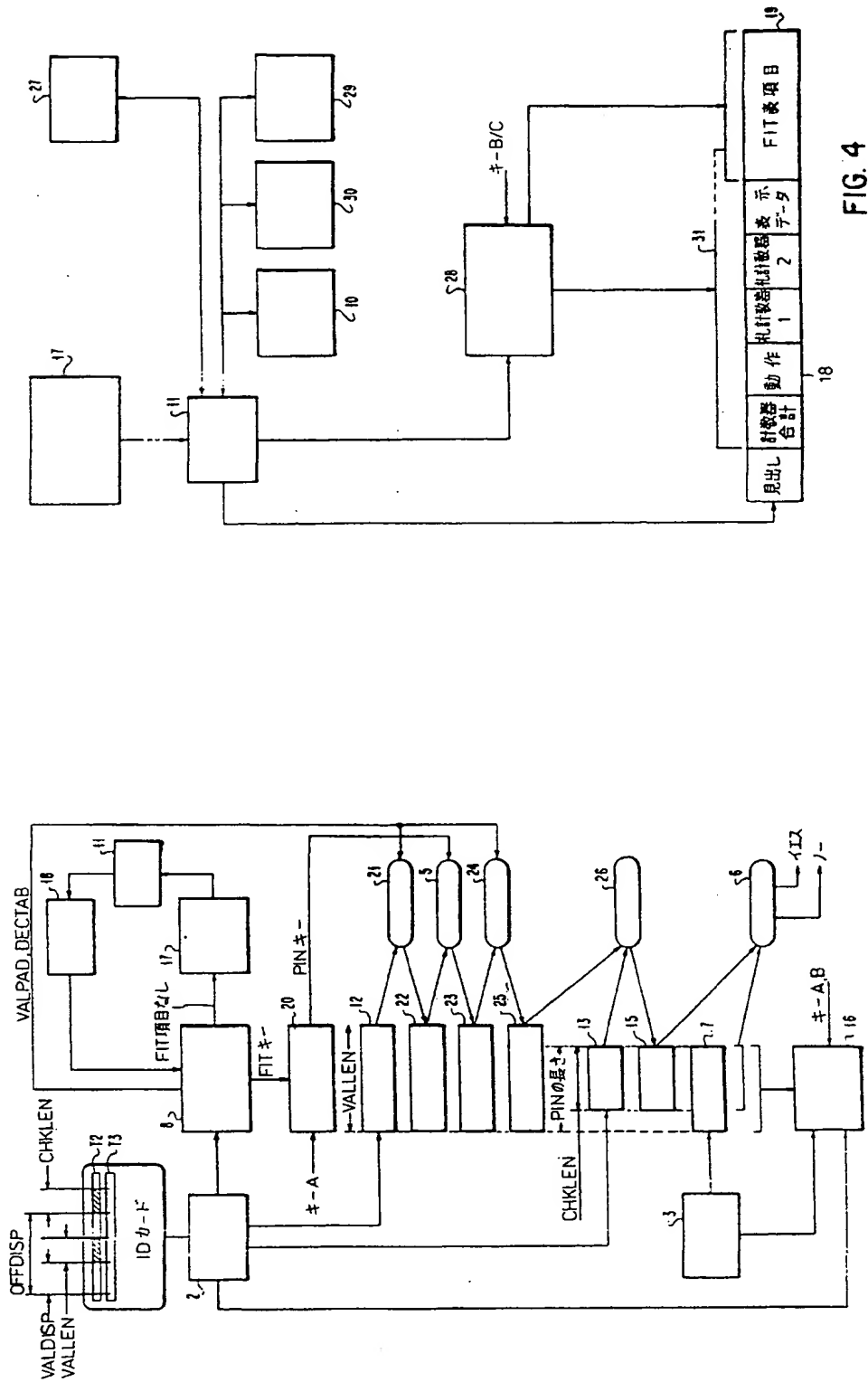


FIG. 4

FIG. 3

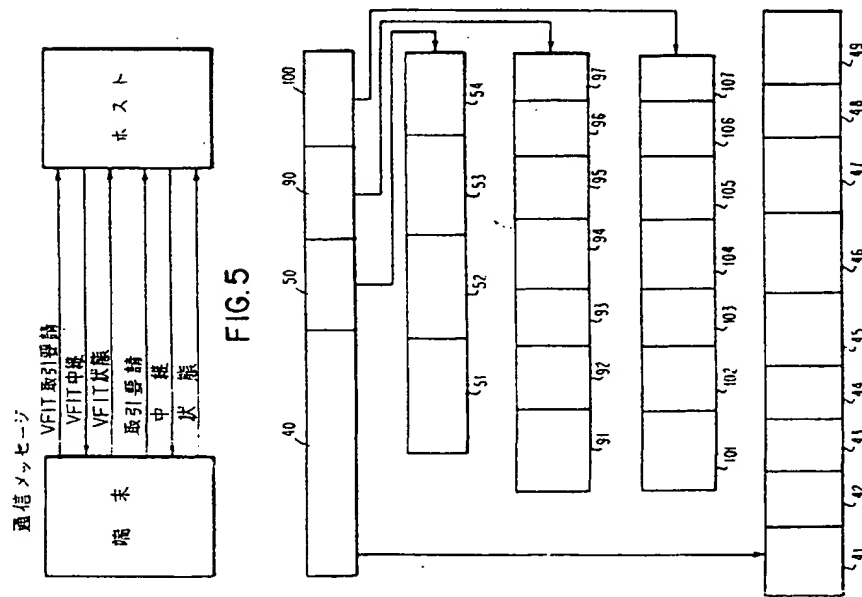


FIG. 5

FIG. 6

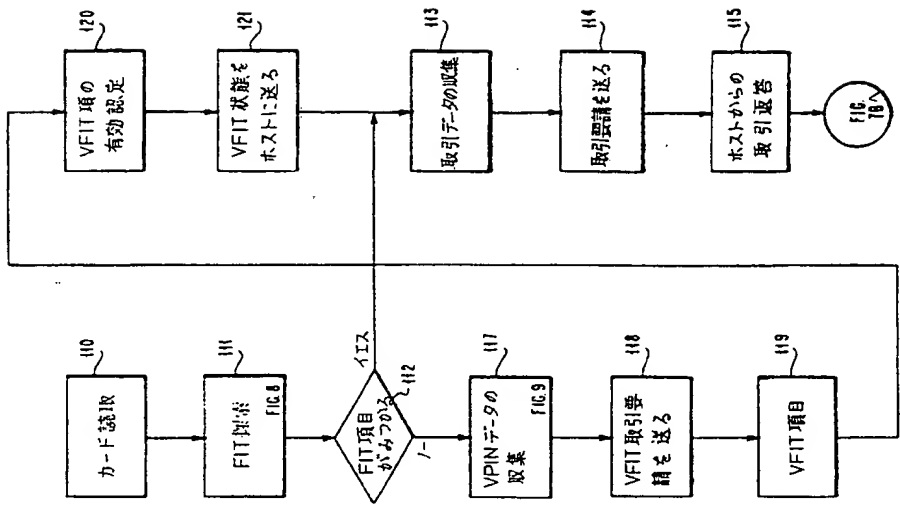


FIG. 7A

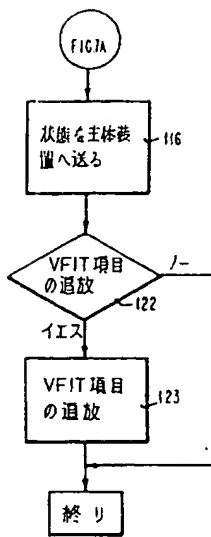


FIG. 7B

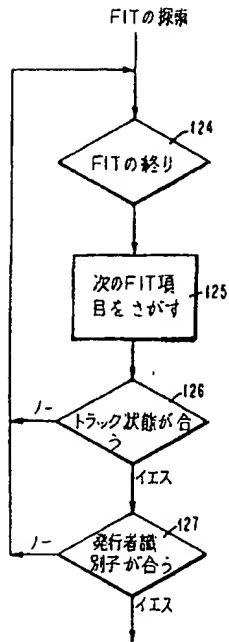


FIG. 8

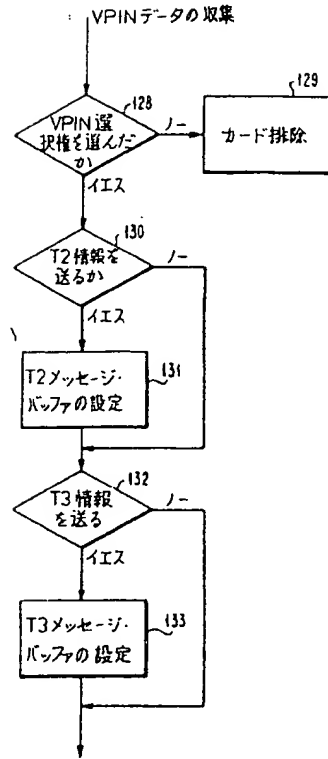


FIG. 9

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.